REMARKS/ARGUMENTS

Claim Rejections – 35 U.S.C. 112

The Examiner has maintained his objection to the use of the term "assertion" and has requested evidence of the fact that the term "assertion" is a well-known and understood term in security and cryptography systems. The following are three links to web sites that show the common use of the term "assertion". A copy of an excerpt from each of these pages is attached to this response.

1. **Glossary for the OASIS Security 2 Assertion Markup Language (SAML) 3 V1.1 4 OASIS Standard, 2 September 2003**

http://www.oasis-open.org/committees/download.php/3401/oasis-sstc-saml-glossary-1.1.pdf

Assertion: A piece of data produced by a SAML authority regarding either an act of authentication performed on a subject, attribute information about the subject, or authorization permissions applying to the subject with respect to a specified resource.

2. **Web Services Federation Language (WS-Federation), Version 1.0, July 8 2003**

http://msdn.microsoft.com/webservices/webservices/understanding/advancedwebservices/default.aspx?pull=/library/en-us/dnglobspec/html/ws-federation.asp

Security Token Service (STS): A security token service is a Web service that issues security tokens (see WS-Security). That is, it makes assertions based on evidence that it trusts, to whoever trusts it. To communicate trust, a service requires proof, such as a security token or set of security tokens, and issues a security token with its own trust statement (note that for some security token formats this can just be a re-issuance or co-signature). This forms the basis of trust brokering.

3. **Vocabularies and Architecture for Implementing Trust in the Semantic Web, Completed, 2004-10-31**

http://www.w3.org/2001/sw/Europe/reports/trust/11.2/d11.2_trust_vocabularies.html

Abstract: This document is a description of an ontological description of a trust assertion, and the implementation in N3 of a trust system for an advanced electronic house scenario.

If further evidence is required, the Examiner is respectfully requested to contact the undersigned by telephone. It is respectfully submitted this is sufficient evidence to establish that the term "assertion" is a well-known and understood term in security and cryptography systems, and the Examiner is respectfully requested to withdraw the 35 U.S.C. 112 rejections.

Claims Rejections – 35 U.S.C. 101

Regarding the 35 U.S.C. 101 rejections, the Examiner, in a telephone interview conducted July 17 and 21, 2005, agreed that the amendments being submitted herewith would overcome the 35 U.S.C. 101 rejections. As such, the Examiner is respectfully requested to withdraw this rejection.

Claims Rejections – 35 U.S.C. 103

The Examiner has withdrawn the previous rejection of the claims under 35 U.S.C. 102(b), and has raised a new rejection under 35 U.S.C. 103(a) of all of the claims as being unpatentable over previously cited Ward et al in view of Hsu et al (U.S. patent No. 5,982,898).

Claim Limitations not Taught

One of the requirements for establishing a *prima facie* case of obviousness is that the references alone or in combination teach all of the limitations of the claims. In applicant's previous response, a detailed discussion was presented of how the limitations of claim 1 were not present in Ward. The Examiner has now conceded that at least the limitation concerning the assertion being between a name and a public key is not taught, and has relied on Hsu for this feature.

Furthermore, applicant maintains that Ward does not teach "selling a pool of unallocated time". The specific text referred to by the Examiner on page 2, lines 15-18 reads:

"Using this system, the motorist is encouraged to purchase a maximum amount of time

on the meter card using his payment card, and is given the assurance that when he returns, he can obtain a refund for any unused time."

The following is an example of how applicant understands this passage.

a) The user has 20$ encoded on his payment card;

b) User goes to park in a spot; rather than paying for 15 minutes, he can pay for the maximum, say 3 hours; Lets say that the cost is 4$ an hour, so 12$ is deducted from his payment card;

c) when he returns after two hours, whatever is left is credited back to his account, in this case 4$.

It can be seen that there is no pool of unallocated time. There is a payment card, for example a bank card, that has some balance in dollars. A payment amount is deducted and then a refund credited.

The Examiner also alleges that Ward teaches "upon request, generating an assertion having a lifetime and subtracting the lifetime from the unallocated time", and has referred to page 4 lines 4-8. As discussed in the previous response, no lifetime is subtracted. Rather, "after the time is selected, the meter computes the value of this time and deducts this amount from the payment card, if possible." See page 4 lines 7-8. Thus, the passage does not teach what the Examiner says it does.

Furthermore, of the two passages in Ward relied upon by the Examiner, in addition to not teaching what is alleged, one of the passages is in the background of the invention section, and the other is in the detailed description. The two pieces are not applied together in Ward.

The Examiner has provided no motivation for combining the Ward and Hsu references. To begin, it is noted that the Hsu and Ward searches do not reference ever a single common class. If experts on searching (in this case the U.S.P.T.O. and the International Searching Authority) do not think the classes were relevant to the other patent then it is hardly likely one skilled in the art would consider searching these two classes. More particularly, Ward references

subclasses of class 235 (registers) while the Hsu references subclasses of class 380 (cryptography). Additionally, Hsu does not mention anything about parking or meters or time; furthermore, Ward does not mention anything about cryptography or security.

It is well established that "There are three possible sources for a motivation to combine references: the nature of the problem to be solved, the teachings of the prior art, and the knowledge of persons of ordinary skill in the art." *In re Rouffet*, 149 F.3d 1350, 1357, 47 USPQ2d 1453, 1457-58 (Fed. Cir. 1998).

As discussed above, the nature of the problem to be solved is completely different in the two references: the teaching of the prior art do not reference each other in any way, and it is unlikely persons of ordinary skill in the art would be aware of knowledge overlapping the two fields.

Furthermore, the proposed modification is not allowed to render the prior art unsatisfactory for its intended purpose. If the proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification. *In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984). In the instant case, modifying the Ward reference to render the assertion to be between a name and a public key would quite obviously render it completely unsatisfactory for parking meter control.

It is respectfully submitted that it has been clearly established that the references do not teach the claim limitations, and furthermore there is no motivation to combine the references. On this basis, the Examiner is respectfully requested to withdraw the rejection of claim 1 under 35 U.S.C. 103(a).

The above arguments apply equally to the remaining claims and as such, the Examiner is respectfully requested to withdraw the rejection of the remaining claims under 35 U.S.C. 103(a) as well. In so doing, Applicant is not conceding that the additional limitations in the remaining claims not discussed herein are in fact taught in the references as alleged by the Examiner.

In view of the foregoing, early favorable consideration of this application is earnestly solicited.

Respectfully submitted,

ROB PARKHILL, ET AL

By _____
Kelly Miranda
Reg. No. 55,960
Tel.: (613) 232-2486 ext. 235

Date: October 21, 2005

RAB:KLM:kbc:rld

OASIS

Glossary for the OASIS Security Assertion Markup Language (SAML) V1.1

OASIS Standard, 2 September 2003

Document identifier:
oasis-sstc-saml-glossary-1.1

Location:
http://www.oasis-open.org/committees/documents.php?wg_abbrev=security

Editor:
Eve Maler, Sun Microsystems (eve.maler@sun.com)
Rob Philpott, RSA Security (rphilpott@rsasecurity.com)

Contributors:
Irving Reid, Baltimore Technologies
Hal Lockhart, BEA Systems
David Orchard, BEA Systems
Zahid Ahmed, formerly of CommerceOne
Tim Moses, Entrust
Joe Pato, Hewlett-Packard
Bob Blakley, IBM
Marlena Erdos, IBM
RL "Bob" Morgan, individual
Marc Chanliau, Netegrity
Prateek Mishra, Netegrity
Darren Platt, formerly of RSA Security
Jahan Moreh, Sigaba
Jeff Hodges, Sun Microsystems

Abstract:
This specification defines terms used throughout the OASIS Security Assertion Markup Language (SAML) specifications and related documents.

Status:
This is an OASIS Standard document produced by the Security Services Technical Committee. It was approved by the OASIS membership on 2 September 2003.

Committee members should submit comments and potential errata to the security-services@lists.oasis-open.org list. Others should submit them to the security-services-comment@lists.oasis-open.org list (to post, you must subscribe; to subscribe, send a message to security-services-comment-request@lists.oasis-open.org with "subscribe" in the body) or use

other OASIS-supported means of submitting comments. The committee will publish vetted errata on the Security Services TC web page (http://www.oasis-open.org/committees/security/).

For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights web page for the Security Services TC (http://www.oasis-open.org/committees/security/ipr.php).

Table of Contents

Term	Definition
Administrator	A person who installs or maintains a system (for example, a SAML-based security system) or who uses it to manage *system entities*, users, and/or content (as opposed to application purposes; see also *End User*). An administrator is typically affiliated with a particular *administrative domain* and may be affiliated with more than one administrative domain.
Anonymity	The quality or state of being anonymous, which is the condition of having a name or identity that is unknown or concealed. **[RFC2828]**
Assertion	A piece of data produced by a *SAML authority* regarding either an act of authentication performed on a *subject*, attribute information about the subject, or authorization permissions applying to the subject with respect to a specified *resource*.
Asserting Party	Formally, the *administrative domain* that hosts one or more *SAML authorities*. Informally, an instance of a *SAML authority*.
Attribute	A distinct characteristic of an object (in SAML, of a *subject*). An object's attributes are said to describe it. Attributes are often specified in terms of physical traits, such as size, shape, weight, and color, etc., for real-world objects. Objects in cyberspace might have attributes describing size, type of encoding, network address, and so on. Which attributes of an object are salient is decided by the beholder. See also *XML attribute*.
Attribute Authority	A *system entity* that produces *attribute assertions*. **[SAMLAgree]**
Attribute Assertion	An *assertion* that conveys information about *attributes* of a *subject*.
Authentication	To confirm a *system entity*'s asserted *principal identity* with a specified, or understood, level of confidence. **[CyberTrust] [SAMLAgree]**
Authentication Assertion	An *assertion* that conveys information about a successful act of *authentication* that took place for a *subject*.
Authentication Authority	A *system entity* that produces *authentication assertions*. **[SAMLAgree]**
Authorization	The process of determining, by evaluating applicable *access control information*, whether a *subject* is allowed to have the specified types of *access* to a particular *resource*. Usually, authorization is in the context of authentication. Once a subject is authenticated, it may be authorized to perform different types of access. **[Taxonomy]**
Authorization Decision	The result of an act of authorization. The result may be negative, that is, it may indicate that the *subject* is not allowed any access to the *resource*.
Authorization Decision Assertion	An *assertion* that conveys information about an *authorization decision*.
Binding, Protocol Binding	An instance of mapping SAML request-response message exchanges into a specific protocol. Each binding is given a name in the pattern "SAML xxx binding".
Credentials	Data that is transferred to establish a claimed principal identity. **[X.800] [SAMLAgree]**

See This in the MSDN Library

Web Services Federation Language (WS-Federation)

Page Options

Version 1.0
July 8 2003

Authors

Siddharth Bajaj, VeriSign
Giovanni Della-Libera, Microsoft
Brendan Dixon, Microsoft
Mike Dusche, Microsoft
Maryann Hondo, IBM
Matt Hur, Microsoft
Chris Kaler (Editor), Microsoft
Hal Lockhart, BEA
Hiroshi Maruyama, IBM
Anthony Nadalin (Editor), IBM
Nataraj Nagaratnam, IBM
Andrew Nash, RSA Security
Hemma Prafullchandra, VeriSign
John Shewchuk, Microsoft

Copyright Notice

Abstract

This specification defines mechanisms that are used to enable identity, account, attribute, authentication, and authorization federation across different trust realms.

Modular Architecture

By using the XML, SOAP and WSDL extensibility models, the WS* specifications are designed to be composed with each other to provide a rich Web services environment. WS-Federation by itself does not provide a complete security solution for Web services. WS-Federation is a building block that is used in conjunction with other Web service and application-specific protocols to accommodate a wide variety of security models.

Status

This WS-Federation Specification is an initial public draft release and is provided for review and evaluation only. BEA, IBM, Microsoft, RSA Security and VeriSign hope to solicit your contributions and suggestions in the near future. BEA, IBM, Microsoft, RSA Security and VeriSign make no warrantees or representations regarding the specifications in any manner whatsoever.

Table of Contents

Signed Security Token - A *signed security token* is a security token that is asserted and cryptographically signed by a specific authority (e.g. an X.509 certificate or a Kerberos ticket)

Proof-of-Possession - *Proof-of-possession* is authentication data that is provided with a message to prove that the message was sent and or created by a claimed identity.

Proof-of-Possession Token - A *proof-of-possession token* is a security token that contains data that a sending party can use to demonstrate proof-of-possession. Typically, although not exclusively, the proof-of-possession information is encrypted with a key known only to the sender and recipient.

Digest - A *digest* is a cryptographic checksum of an octet stream.

Signature - A *signature* is a value computed with a cryptographic algorithm and bound to data in such a way that intended recipients of the data can use the signature to verify that the data has not been altered since it was signed by the signer.

Security Token Service (STS) - A *security token service* is a Web service that issues security tokens (see WS-Security). That is, it makes assertions based on evidence that it trusts, to whoever trusts it. To communicate trust, a service requires proof, such as a security token or set of security tokens, and issues a security token with its own trust statement (note that for some security token formats this can just be a re-issuance or co-signature). This forms the basis of trust brokering.

Attribute Service - An *attribute service* is a Web service that maintains information (attributes) about principals within a trust realm or federation. The term principal, in this context, can be applied to any system entity, not just a person.

Pseudonym Service - A *pseudonym service* is a Web service that maintains alternate identity information about principals within a trust realm or federation. The term principal, in this context, can be applied to any system entity, not just a person.

Trust - *Trust is* the characteristic that one entity is willing to rely upon a second entity to execute a set of actions and/or to make set of assertions about a set of subjects and/or scopes.

Trust Domain/Realm - A *Trust Domain/Realm* is an administered security space in which the source and target of a request can determine and agree whether particular sets of credentials from a source satisfy the relevant security policies of the target. The target may defer the trust decision to a third party (if this has been established as part of the agreement) thus including the trusted third party in the Trust Realm.

Validation Service - A *validation service* is a Web service that uses the WS-Trust mechanisms to validate provided tokens and assess their level of trust (e.g. claims trusted).

Direct Trust - *Direct trust* is when a relying party accepts as true all (or some subset of) the claims in the token sent by the requestor.

Direct Brokered Trust - *Direct Brokered Trust* is when one party trusts a second party who, in turn, trusts or vouches for, the claims of a third party.

Indirect Brokered Trust - *Indirect Brokered Trust* is a variation on direct brokered trust where the second party can not immediately validate the claims of the third party to the first party and negotiates with the third party, or additional parties, to validate the claims and assess the trust of the third party.

Signature validation - *Signature validation* is the process of verifying that the message received is the same as the one sent.

Sender Authentication - *Sender authentication* is corroborated authentication evidence possibly across Web service actors/roles indicating the sender of a Web service message (and its associated data). Note that it is possible that a message may have multiple senders if authenticated intermediaries exist. Also note that it is application-dependent (and out of scope) as to how it is determined who first created the messages as the

Vocabularies and Architecture for Implementing Trust in the Semantic Web

Project name:
Semantic Web Advanced Development for Europe (SWAD-Europe)
Project Number:
IST-2001-34732
Workpackage name:
11. Trust
Workpackage description:
http://www.w3.org/2001/sw/Europe/plan/workpackages/live/esw-wp-11.htm
Deliverable title:
11.2: Implementation of a Trust System
URI:
http://www.w3.org/2001/sw/Europe/reports/trust/11.2/d11.2_trust_vocabularies.ht
Authors:
Alvaro Arenas, CCLRC, UK
Brian Matthews, CCLRC, UK
Michael Wilson, CCLRC, UK
Jan Grant, ILRT, University of Bristol

Abstract:
This document is a description of an ontological description of a trust assertion, and the implementation in N3 of a trust system for an advanced electronic house scenario.
Status:
Completed, 2004-10-31.
Version:
Comments on this document are welcome and should be sent to Brian Matthews

---

Contents
